CLAIMS

1. Method of inserting a message into digital data representative of physical quantities, the message including ordered symbols, including the steps of:

- segmenting (E2) the data into regions,
- associating (E3) at least one region with each symbol to be inserted,

characterised in that, for each region into which a symbol in question is to be inserted, it includes the steps of:

- determining (E7) a pseudo-random function, from a key which depends:
  - on an initial key, and
  - on the length of the message,
- modulating (E8) the symbol in question by the previously determined pseudo-random function in order to supply a pseudo-random sequence,
- adding (E10) the pseudo-random sequence to the region in question.

2. Insertion method according to Claim 1, characterised in that the dependence of the key as regards the length of the message is provided by the dependence of the key as regards:

- the number of times the symbol to be inserted has already been inserted into other regions, and
- the ranking of the symbol among the ordered symbols.

3. Insertion method according to Claim 1 or 2, characterised in that it includes a prior step (E1) of transformation of the digital data by a reversible transformation.

4. Method for extracting a message from digital data representative of physical quantities, the message including ordered symbols, including the steps of:

- segmenting (E210) the data into regions,

- extracting (E21) the length of the inserted message,

- extracting (E22) the inserted message.

5. Extraction method according to Claim 4, characterised in that extracting the length of the inserted message includes the steps of:

- selecting (E211) a set of length values, and

- calculating (E217) a correlation between the message and the digital data, for each of these values,

- determining (E223) a local maximum among the correlation values.

6. Extraction method according to Claim 4 or 5, characterised in that extracting the length of the inserted message is carried out while processing F times fewer coefficients than the digital data include.

7. Extraction method according to Claim 6, characterised in that it includes the steps of:

- determining (E22) the total number of coefficients (C) to be considered,

- selecting (E26, E27) a maximum number of coefficients corresponding to a same inserted symbol, then, if the total number of coefficients to be considered has not been reached,

- reiterating (E29) the selection step, for another symbol.

8. Device for inserting a message into digital data representative of physical quantities, the message including ordered symbols, including:

- means (3) for segmenting the data into regions,

- means (5) for associating at least one region with each symbol to be inserted,

characterised in that, it includes:

- means (7) for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends:

- on an initial key, and

- on the length of the message,

- means (8) for modulating the symbol in question by the previously determined pseudo-random function in order to supply a pseudo-random sequence,

- means (5) for adding the pseudo-random sequence to the region in question.

9. Insertion device according to Claim 8, characterised in that the means (7) for determining a pseudo-random function are configured in such a way that the dependence of the key as regards the length of the message is provided by the dependence of the key as regards:

- the number of times the symbol to be inserted has already been inserted into other regions, and

- the ranking of the symbol among the ordered symbols.

10. Insertion device according to Claim 8 or 9, characterised in that it includes means (2) for prior transformation of the digital data by a reversible transformation.

11. Device for extracting a message from digital data representative of physical quantities, the message including ordered symbols, including:

- means for segmenting the data into regions,

- means (22) for extracting the length of the inserted message,

- means (23) for extracting the inserted message.

12. Extraction device according to Claim 11, characterised in that the means (22) for extracting the length of the inserted message include:

- means for selecting a set of length values, and

- means for calculating a correlation between the message and the digital data, for each of these values,

- means for determining a local maximum from among the correlation values.

13. Extraction device according to Claim 11 or 12, characterised in that the means for extracting the length of the inserted message are configured to perform the extraction while processing F times fewer coefficients than the digital data include.

14. Extraction device according to Claim 13, characterised in that it includes:

- means for determining the total number of coefficients (C) to be considered,

- means for selecting a maximum number of coefficients corresponding to a same inserted symbol,

- means for reiterating the processing of the selection means, for another symbol, if the total number of coefficients to be considered has not been reached.

15. Insertion device according to any one of Claims 8 to 10, characterised in that the segmentation, association, determination, modulation and addition means are incorporated into:

- a microprocessor (100),

- a read-only memory (102) including a program for processing the data, and

- a random-access memory (103) including registers suitable for recording variables modified in the course of the running of the said program.

16. Extraction device according to any one of claims 11 to 14, characterised in that the segmentation and extraction means are incorporated into:

- a microprocessor (100),

- a read-only memory (102) including a program for processing the data, and

- a random-access memory (103) including registers suitable for recording variables modified in the course of the running of the said program.

17. Apparatus (10) for processing a digital image, characterised in that it includes means suitable for implementing the method according to any one of claims 1 to 7.

18. Apparatus (10) for processing a digital image, characterised in that it includes the device according to any one of Claims 8 to 16.

19. Storage medium storing a program for inserting according to any one of claims 1 to 3.

20. Storage medium according to claim 17, characterized in that it is detachably mountable on a device according to any one of claims 8 to 10.

21. Storage medium according to claim 19, characterized in that it is a floppy disk or a CD-ROM.

22. Computer program on a storage medium and comprising computer executable instructions for causing a computer to insert according to any one of claims 1 to 3.

23. Storage medium storing a program for extracting according to any one of claims 4 to 7.

24. Storage medium according to claim 23, characterized in that it is detachably mountable on a device according to any one of claims 11 to 14.

25. Storage medium according to claim 23, characterized in that it is a floppy disk or a CD-ROM.

26. Computer program on a storage medium and comprising computer executable instructions for causing a computer to extract according to any one of claims 4 to 7.